Systematic Literature Review on Risk Management Models for Cyber-Physical System Resilience Across Various Sectors: Attacks, Methods, Gaps.

Subairu, S.O., Hashimu, A., Suleiman, A., Noel, M.D. & Adamu, A.M.
Department of Cyber Security Science,
Federal University of Technology,
Minna, Niger State, Nigeria
E-mails: sikiru.subairu@futminna.edu.ng, attahiruhmte25266@st.futminna.edu.ng,
ahmads@futminna.edu.ng, moses.noel@futminna.edu.ng,
mohammedaamte25278@st.futminna.edu.ng

ABSTRACT

Cyber-Physical Systems (CPS) have become the foundation of modern critical infrastructure, these includes power grid, water facility, transportation, agriculture, manufacturing, and healthcare systems. However, deep integration of cyber and physical components has increased the attack rate, leaving these domains vulnerable to sophisticated attacks capable of causing severe physical harm. This research gives a systematic literature review of risk management strategies for CPS resilience across different industries, using the PRISMA approach. This systematic literature review evaluates 1,247 peer-reviewed articles published between 2022 and 2026 that investigate risk management methods for CPS resilience across diverse sectors. Out of these 1247, 47 were selected for this review. We identified five major thematic clusters: (1) risk assessment methodologies; (2) attack detection and defense mechanisms; (3) resilience frameworks and metrics; (4) cascading failure analysis; and (5) sector-specific applications of these models. Our findings show that conventional risk management approaches often fail to handle the cyber-physical interdependence that distinguishes modern CPS. Furthermore, we have identified and categorized important attack types, adversarial tactics, proposed detection and mitigation strategies, and persistent vulnerabilities in the existing literature. Our findings indicated that while deep learning and anomaly detection approaches dominate current research, there are substantial gaps in proactive mitigation, explainable AI, real-world validation, and human factor integration. We also noticed an increasing emphasis on dynamic, real-time risk assessment approaches that use artificial intelligence and machine learning, as well as an increased focus on socio-technical and environmental aspects. This analysis provides a consolidated taxonomy of risk management methodologies, identifies significant research gaps, and suggests an integrative framework for CPS resilience engineering.

Keywords: Cyber-Physical Systems, Risk Management Methodology, CPS Resilience, Explainable AI, Critical Infrastructure.

CISDI Journal Reference Format

Subairu, S.O., Hashimu, A., Sulieman, A., Noel, M.D., Adamu, A.M. (2026): Subairu, S.O., Hashimu, A., Suleiman, A., Noel, M.D. & Adamu, A.M.. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 17 No 3, Pp 63-76. Available online at www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V17N3P4

1. INTRODUCTION

1.1 Background and Motivation.

Cyber-Physical System (CPS) is a system that combines computing algorithms and communication networks with physical processes, forming the foundation of modern Critical Infrastructure (Huang *et al*., 2025). These includes smart grids that power our cities and water treatment plants that ensure public health, autonomous vehicles that reshape transportation, and medical implants that monitor patient health. However, the digital transformation has resulted in unmatched vulnerabilities. Unlike attacks against Information Technology (IT) which generally compromises confidentiality and integrity of data, cyber-physical attacks can have immediate and devastating physical consequences. Past incidents such as the 2015 Ukrainian power grid attack and the Colonial pipeline ransomware attack in 2021, are both examples of how attacks on CPS could disrupts an entire nation and cause significant economic loss (Huang *et al*., 2025; Khattak, 2024).

Industrial sectors have transformed digitally which led to accelerated adoption of CPS in some specific domains of critical infrastructure. CPS (combined physical processes with computational and communication components) are the heart of "Industry 4.0 projects" (Chae *et al*., 2023). CPS is capable of "real-time monitoring and control, optimization of complex activities ranging from smart power grids to autonomous transportation networks" (Jiang *et al*., 2023). However, this integration has created substantial cybersecurity flaws. High-profile incidents, such as the Stuxnet attack in 2010 targeted at the Iranian nuclear facility and the 2021 Colonial Pipeline ransomware incident all reminds us that "cyber-physical attacks can cause significant physical damage and societal disruption" (Mekdad *et al*., 2021; Kumar et al., 2022).The consequences of a compromise CPS can be widely felt in physical and cyber environments, such as equipment damage, environmental damage, and harmful impacts on human safety, unlike traditional IT systems (Jiang *et al*., 2023).

Awareness of these risks has increased which led to significant research on risk management techniques that are fit for CPS characteristics. CPS risk management is different from conventional risk assessment schemes for pure IT or pure physical systems as it involves various characteristics like real-time requirements, legacy integration, cyber-physical interdependence, and complex failure propagation (Cassottana *et al*., 2023).

For this reason, it is now essential to make a paradigm shift from conventional security to resilience. Resilience can be defined as the ability to predict, withstand, recover from, or adjust to dangerous Cybersecurity events. Cybersecurity on the order hand deals with protecting against those events (Alrumaih & Alenazi, 2025; Aghazadeh *et al*., 2024). Therefore, risk management in the context ofCPS-resilience requires an all-encompassing approach that involves organizational governance, physical process control, cyber protection and human aspects.

Despite significant research in a number of industries including water and power sectors, the literature is still scattered with each domain creating its own taxonomy, detection and mitigation techniques. Agreement between researchers and practitioners about viable attack countermeasures and research gaps across industry boundaries still remains unclear.This systematic review fills this gap as it provides a comprehensive and cross-sectoral examination of risk management strategies for CPS resilience. "Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)" technique was used to ensure rigor, transparency, and repeatability.

1.2 Objectives and Contributions.

This systematic literature review seeks to;

1. Identify and categorize risk management models for CPS resilience in different industries.
2. Review risk assessment, attack detection and enhancement of resilience approaches.
3. Evaluate the effectiveness and limitations of the current approaches.
4. Synthesize findings to identify research gaps and recommend future direction.

The remaining sections are organized as follows: section 2 reviews related work, section 3 describes PRISMA-based methodology, section 4 presents the results, including a complete taxonomy of risk methodologies, methods, mitigation strategies, and vulnerabilities across sectors. Section 5 discusses findings and suggests research gaps specific to some domains as future directions. Furthermore, section 6 discusses constraints and potential scope. Section 7 concludes the paper.

2. RELATED WORKS

Several surveys have investigated CPS security and resilience from a variety of perspectives. A comprehensive study carried out by Huang *et al*., (2025) to review the "cyber-physical security challenges in new power system". Their review focused on integrating "Generation-Grid-Load-Storage (GGLS)" and "Sensing-Transmitting-DecisionMaking-Controlling (STDC) loop". Similarly, Feng *et al*., (2024) reviewed "coordinated attacks on cyber-physical power systems" and characterized it as either "Coordinated Cyber-Physical Attack" or "Coordinated Cyber Attacks (CCA)" and conducted a comprehensive analysis of detection and mitigation plans. In the industrial control systems (ICS) domain, Canonico *et al*. (2025) developed anomaly-based techniques to threat identification using deep learning, proving the efficacy of autoencoders, LSTMs, and GANs on the SWaT dataset.

ERINDA was suggested by Alrumaih and Alenazi, (2025), a framework that enhances the resilience of Industrial Control System (ICS) to Distributed Denial of Service (DDoS) attack by combining both proactive and adaptive response strategies. Water sector has also attracted serious attention. Homaei *et al*. (2026) developed the Causal Digital Twins (CDT) for water systems with F1 score of 94.4% on the SWaT dataset. Atat *et al*. (2023) proposed the graph partitioning approaches based on typed-graphlets to avoid cascade failures in water distribution systems. Machaka *et al*. (2025) developed virtual ICS testbeds to test the threats posed by Modbus/TCP protocol to wastewater treatment plants.

Cybersecurity vulnerabilities in cooperative driving automation in the transportation sector was analyzed by Khattak (2024). They found out that fake Basic Safety Message (BSM) attacks increased volatility by 35-50% and emissions by 20%. Rehman *et al*. (2026) proposed a set of machine learning-powered solutions for detecting eclipse attacks in Ethereum network with an F1 score of 96%. Several cross-sectoral surveys have been done. There are a number of cross-sectoral surveys conducted. Kampourakis *et al*. (2023) systematically reviewed the security testbeds over wireless technologies that have been used in CPS within water, healthcare, transportation, agricultural, energy and maritime applications. Furthermore, Abshari and Sridhar (2025) evaluated anomaly detection techniques and categorizes them into four types; data and model-driven, hybrid and system-oriented approaches. Aghazadeh *et al*. (2024) did a study on risk assessment for cyber resilience, defining techniques, standards, and legislation.

Despite these significant contributions, some gaps remain. First, existing surveys are usually narrow in scope, or they are limited to specific technical approaches and do not really provide a comprehensive cross-sectoral view. Second, most studies focus on detection, and not enough on proactive mitigation and recovery which are key to resilience. Third, the human aspect is poorly considered in technical surveys, as is the case for trust, the blame attribution, and operators' decision making. Fourth, there is gap between translating research findings into meaningful domain-specific gaps. To address these gaps, we conducted a review of published papers that focused on 47 papers from eight sectors, explicitly categorized attacks, methods, solutions, and weaknesses, included technical, organizational and human factors, and made concrete, domain-specific research recommendations based on gaps identified.

3. METHODOLOGY

This SLR adheres to the PRISMA 2020 statement to ensure transparency, completeness, and reproducibility. The process consisted of four steps: identification, screening, eligibility, and inclusion as shown in figure 1.

The review was guided by the following Research Questions (RQs):

RQ1: What risk assessment methodologies were proposed for CPS across different sectors?
RQ2: How do existing approaches address attack detection and mitigation in CPS environments?
RQ3: What frameworks and metrics exist for quantifying CPS resilience?
RQ4: How are cascading failures modeled and analyzed in interdependent cyber-physical systems?
RQ5: What are the primary research gaps and future directions in CPS risk management?

3.1 Search Strategy

Thorough search was carried out from four digital libraries; 'IEEE Xplore', 'ScienceDirect', 'Scopus', and 'ACM digital library'. The rational was that they are "reputable and reliable repositories of academic literature, each with an extensive collection of publications relevant to cybersecurity" domain, (Rehman *et al*. 2026). We focused primarily on search string that has three keyword families related to our literature review:

1. ("CPS," OR "cyber-physical system" AND "Risk management model" OR "risk assessment framework" AND "machine learning" OR "deep learning").
2. ("Critical infrastructure" AND "resilience" AND "attack" OR "threat" OR "intrusion detection" AND "digital twin" OR "game theory").
3. ("industrial control system" OR "smart grid" OR "critical infrastructure" AND "anomaly detection" OR "IDS" OR "attack detection" AND "machine learning").

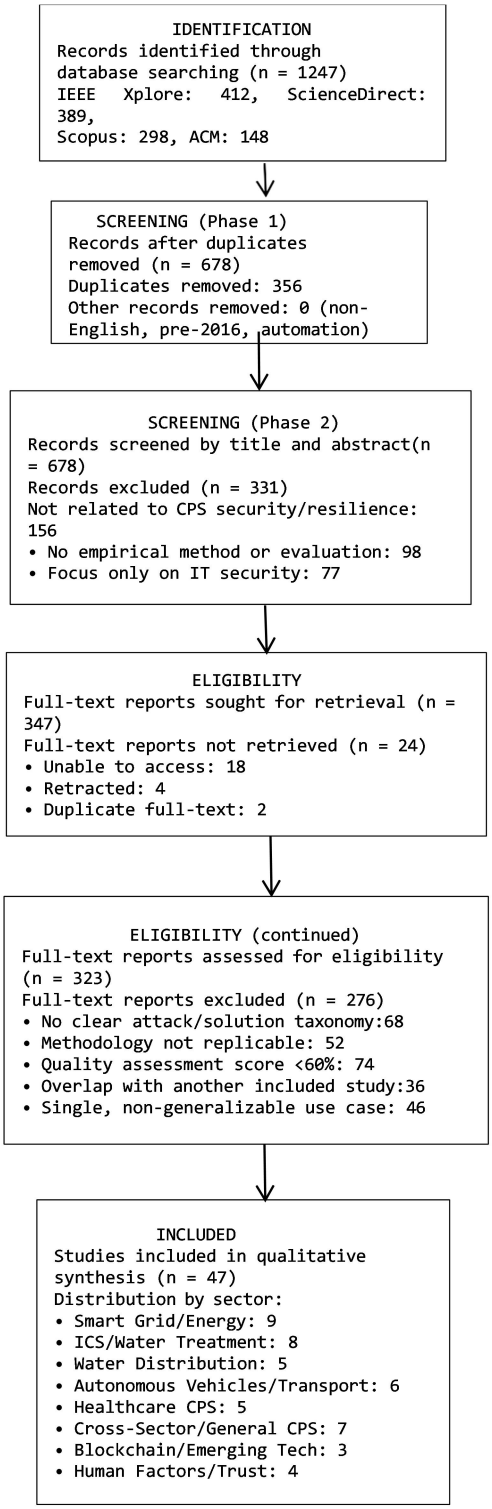


Figure 1: PRISMA Flow Diagram

3.1 Screening and Eligibility Criteria

The screening of the articles is as follows:
Inclusion criteria;

1. Relevance: Directly addresses CPS security, resilience, and risk management.
2. Empirical content that either proposes, implements, or assesses a particular method, model, or framework.
3. At least one important infrastructure sector (e.g energy, water, transport, healthcare, ...etc).
4. Peer-reviewed journals.
5. English Language articles and conference papers published between 2022-2026.

Exclusion criteria;

1. Non-English publications.
2. Commentaries, book reviews, or short summaries without empirical relevance.
3. Studies that only focused on IT security with little attention to physical processes.
4. Duplicated publications.

1247 articles proceeded to full-text review after screening titles and abstracts. Following full-text assessment against eligibility criteria, 47 articles were selected for final inclusion as indicated in the PRISMA flow diagram in figure 1 above.

3.2 Data Extraction and Synthesis.

A template was designed to extract data. It collected the following information:

1. Bibliography: (Author(s), year, title, source).
2. Sector/domain: (energy, water, transportation, healthcare, cross-sector).
3. Attack type(s) and vectors.
4. Proposed detection or mitigation method(s).
5. The dataset or testbed employed.
6. Reported performance metrics.
7. Identified limitations and weaknesses.

Data extraction was done independently by two reviewers and differences were resolved by discussion. The information retrieved was qualitative and quantitative performance indicators were also given.

3.3 Quality Assessment.

All included studies were assessed on quality using a modified version of the “Critical Appraisal Skills Programme (CASP)” checklist for systematic reviews assessing:

1. Highly stated research aims and problem formulation
2. Appropriateness of method to research questions
3. Validity of the experimental design and choice of data.
4. Performance assessment and analysis.
5. Scope assumption and limitation.

The studies with a score below 60% on the quality assessment were excluded, resulting in 47 high-quality studies.

4. RESULTS

Figure 2 illustrates the number of publications published each year. The output during 2022 and 2023 was steadily increasing although it was still modest, averaging at 2-7 articles per year. This began to rise significantly in 2023 and has seen considerable growth up to 2025 and 2026. The rise can be ascribed to heightened awareness of security risks in CPS and increasing research investment in these areas.

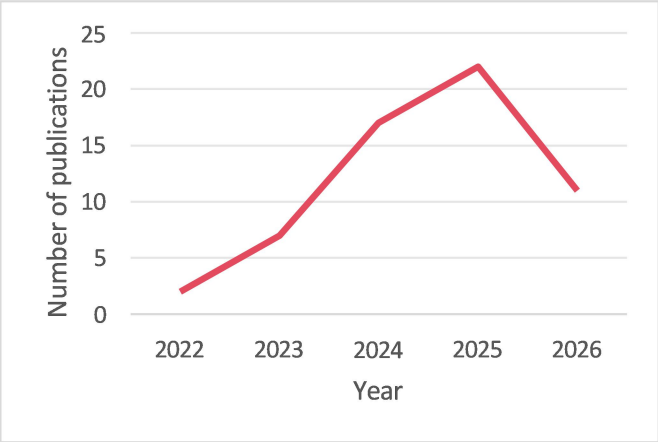


Figure 2. Publication Distribution by Year.

A spike in publications is in line with some of the previous major cyber-physical attacks. Some of these include NotPetya attack 2017, the 2019 Venezuela blackout, 2021 Colonial Pipeline incident and the Ukrainian power grid attack from 2015-2016 (Kumar *et al*., 2022; Jiang *et al*., 2023). In the following subsections, we show how these studies helped to answer the research questions posed earlier in this research.

RQ1: What risk assessment methodologies from the existing literatures have been proposed for CPS across different sectors?

I. Qualitative and Semi-Quantitative Approaches:

Conventional threat modeling approaches have been adapted for CPS contexts. Khan *et al*. (2017) extended "Microsoft's STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)" methodology on CPS, demonstrating its application to smart grid systems. Similarly, Kim *et al*. (2022) combined STRIDE with "DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability)" evaluation of distributed control systems in oil refineries.

However, these approaches face limitations in CPS contexts. Huang *et al*., (2025) pointed out that Data Flow Diagrams in STRIDE are not always sufficient to represent cyber-physical interactions, and that the threat "severity of compromise in CPS extends beyond the six threat categories". This issue was addressed by Valenza *et al*., (2022) with a "hybrid threat model for smart systems" that combines the safety and security perspectives.
For the vulnerability prioritization in CPS, the Common Vulnerability Scoring System (CVSS) is still

widely used (Stergiopoulos *et al*., 2022). There had been criticism on CVSS for its non-completeness in terms of the operating conditions of the industrial environment or the physical effects of exploiting the vulnerability (Amro *et al*., 2023).

II. Quantitative Risk Assessment Models:

There has been a shift in emphasis to quantitative approaches to aid in risk-informed decision making. Following this, Lyu *et al*. (2022) introduced a Bayesian network-based C2P (Cyber-to-Physical) risk assessment framework that they applied to CPS, in which cyber-attacks can escalate to physical impacts. Amro *et al*. (2023) presented an autonomous passenger ship approach to fuse the "Failure Modes Effects and Criticality Analysis (FMECA)" and the "MITRE ATT&CK Framework". This combination offers systematic attack path identification and access to the full knowledge of adversary tactics embedded in ATT&CK. In 2023, Zhang and Ni proposed a method to evaluate the security risk of cyberattack on distribution systems considering both cyber and physical impacts. They propose a method based on the maximum exploiting probability models to determine high risk substations.

III. Graph-Based and Network Models:

The idea of attack graphs and attack trees have been extensively used for CPS risk assessment. Stergiopoulos *et al*. (2022) introduced a tool named CPSRA (Cyber-Physical Systems Risk Assessment) which generates isomorphic graphs of CPS process models and then uses graph algorithms to detect high complexity structure components and attack paths. Their method involves incorporating real-life CVEs to automatically support decision making related to resilience improvement.

Within Smart grid wide area monitoring, Paudel *et al*. (2017) created attack models that are focused on the Advanced Persistent Threats (APT) with the help of attack trees for representing multi-stage attack scenarios. Following the similar concepts, Du *et al*. (2024) created a "cyber-attacks targeting converter-driven stability" mechanism of power grid with "PMSG-based wind farms". Iturbe *et al*. (2024) proposed a "multi-layered approach" which uses "threat modeling and attack simulation", in order to be able to do "security assessment" at various levels of abstraction.

IV. Dynamic and Real-Time Risk Assessment:

The traditional approaches to risk assessment generally involve a periodic exam or one at design. The cyber world, however, is a constantly changing environment, and CPS operations are as well, requiring the flexibility to respond to new threats in real time. Cheimonidis and Rantos (2025) proposed a novel dynamic risk assessment that combines both Exploit Prediction Scoring System (EPSS) and Bayesian Network. Their method is proactive, making estimates on the likelihood of vulnerability being exploited over a 30-day horizon, with real-time threat intelligence. Cao *et al*. (2025) proposed a quantitative evaluation framework of resilience by introducing a Markov chain-based cyber-layer anomaly modeling and physical-domain performance degradation modeling. By this method, one can achieve dynamic resilience assessment via cyber-physical coupling and generation of performance curve.

RQ2: How do existing approaches address attack detection and defense in CPS environments?

I. Model-Based Detection:

Model-based detection approaches use mathematical models of physical processes to discover abnormalities. These techniques are based on the theory of comparing real system activities with the predicted system activities from the system models to identify the anomalies as possible attacks. Jiang *et al*. (2023) summaries' the control-theoretic techniques such as watermarks, residuals and observers that enable watermark detection. Zografopoulos and Konstantinou (2022) designed detection techniques for autonomous cyber-physical inverter-based microgrids to detect stealthy attacks using model-based techniques.

II. Machine Learning and Deep Learning Detection:

In Machine Learning, detection has been gaining significant momentum in the domain of attack detection especially on identifying unknown, or zero days, attacks that are not covered by the signatures.Kaliyaperumal *et al*. (2025) proposed a hybrid deep learning intrusion detection system (IDS) for Agriculture 4.0. They used deep autoencoders and HDBSCAN for binary and multiclass classification of the detected intrusion respectively. They were able to get 99.06% accuracy on CIC-DDoS2019 data set and proved that their method was efficient in securing agricultural cyber-physical system.

Soomro *et al*. (2024) introduced a lightweight federated deep intrusion detection system (FedSecureIDS) for industrial CPS, and in 2024 they proposed the same approach for industrial CPS. They use “CNNs, LSTMs, and MLPs” together with “federated learning” to train collaboratively without sharing sensitive data and employ lightweight symmetric cryptography for the communication security. Presekal *et al*. (2023) proposed a hybrid model of GC-LSTM and CNN to improve cyber situational awareness and detect early-stage attacks for cyber monitoring and detection in power grids via communication-based anomaly analysis to detect cyber threats in real-time. Canonico *et al*. (2025) compared a number of unsupervised anomaly detection models (AE, AE-LSTM, VAE, GAN) on both network and physical information from a real-world CPS testbed. They showed that multiple models are better suited for analyzing different kinds of data, which means multi-source analysis is required for comprehensive detection.

III. Defense and Mitigation Strategies.

There are two types of defense strategy; Proactive and Reactive. Proactive solutions involve access control, network segmentation, encryption, and move-on-the-targets. Reactive measures contain resilient state estimation, control reconfiguration and fault-tolerant control.Liu *et al*., (2024) put forward a “resilience framework for power electronic systems” that can resist and recover power electronics systems from cyber-physical attacks.he framework is organized into four stages: “Anticipate and Prepare, Resist and Absorb, Detect and Assess, Recover”. Sobb and Turnbull (2025) examined the 2024 CrowdStrike outage from the perspective of Complex Cyber-Physical-Social Systems to show that systems being connected and homogeneous can magnify the impact of single point failures.

RQ3: *What frameworks and metrics exist for quantifying CPS resilience?*

I. Quantitative Resilience Metrics:

Longo *et al*. (2025) have carried out an extensive literature review on the evolution of cyber-physical resilience, examining existing definitions, indicators and legal aspects. After analyzing 360 documents through bibliometric analysis, they found that the definitions of resilience have shifted from static models of robustness to dynamic, adaptive, and systemic models, that include cyber-physical complexity. Umunnakwe *et al*. (2021) proposed ranking cyber-physical components based on betweenness centrality, allowing the identification of important components whose failure would have the greatest impact on the system's durability.

II. Resilience Engineering Frameworks

Several different engineering models have been suggested for CPS. Idaho National Laboratory has developed a "Consequence-Driven Cyber-Informed Engineering (CCE)" framework, which focuses on determining critical functions and providing for cyber-resilience against advanced adversaries (Liu *et al*., 2024; Assante *et al*., 2019). The NIST Cybersecurity Framework (CSF) 2.0 offers guidance for the cybersecurity of critical infrastructure, and the IEC 62443 series, "Industrial Automation and Control Security," covers security for industrial automation and control systems (Longo *et a*l., 2025).

III. Cyber-Physical-Social Resilience

New studies indicate that the resilience of CPS cannot be achieved through technology. In their work, Segovia-Ferreira *et al*. (2024) investigate cyber-resilience strategies for cyber-physical systems, including diversity, segmentation, moving target defenses, and game theory. Sobb *et al*. (2025) described "responsible resilience" as "the ability of systems to adapt to cyber risks through trustworthy, transparent agent-based models in socio-technical contexts". The E3R paradigm is operationalized via integrated modelling approaches to comprehensive cyber resilience, and it is being developed by their team.

RQ4: *How are cascading failures modeled and analyzed in interdependent cyber-physical systems?*

I. Interdependencies and Propagation Mechanisms

In CPS, cascading failures that propagate through interdependent cyber and physical components are of great concern. Su *et al*. (2024) studied cascading failure in mine CPS and presented a state transfer model based on multiple operational states and uncertainty theory to describe the variations of reliability. The study by He *et al*., (2024) offers in-depth review of cascading failure in CPS. It covers failure modeling techniques and vulnerability analysis methods.They also found non-linear propagation patterns driven by the interdependence between the cyber and physical layers, which conventional models do not capture.

II. Modeling Approaches

Zhang and Chen (2024) in their paper developed "an integrated modeling framework for cascading failure analysis and speed assessment of cyber-coupled power grids:". Their method is power flow analysis and modelling of dependency in the cyber layer. Ding *et al* (2024) considered "combined nature of cyber-physical power systems" and studied the effect of coupling methods on preserving cascaded failures from different attack scenarios.

III. Resilience Enhancement Strategies

Chen *et al*. (2020) analyzed the issue of "protection strategies for active defense in cyber-physical power systems", which is related to the survival of interdependent clusters in the event of cascading failures. They found that, by keeping their subsystems intact but not interdependent, the whole system could not collapse. Recently, Gao *et al*. (2021) discussed the impact of wind power variability in “cascading failures in cyber-physical power systems”, which illustrates the extra complexity that the integration of renewable energy brings to failure propagation analysis.

RQ5: What are the primary research gaps and future directions?

1. **1.Integration of Threat and Attack Modeling.** In the literature, the terms “threat modeling” as well as “attack modeling” are often used without clear definitions and relations between them (Huang *et al*. 2025). Most research has tended to concentrate on threat modelling during early design stages and attack modelling during operational stages has received little attention.
2. **Dynamic and Real-Time Assessment.** Few approaches currently exist that offer true real-time risk assessment capabilities, which dynamically adjust to threat landscapes and system states. In an attempt to address this problem, Cheimonidis and Rantos (2025) added Exploit Prediction Scoring System but limited its inclusion.
3. **Socio-Technical Integration.** Social factors (consumer behavior, policy, operator decisions) have a significant effect on the risk in the CPS, but most models either do not consider them as dynamic constituents or assume they are fixed inputs.
4. **Cross-Sector Generalization.** Most studies are single sector (especially energy) and limited validation of approaches across different CPS domains.
5. **Validation and Benchmarking.** Only a few studies are available that validate on real-world systems or standardized benchmarks. Most evaluations are performed on simulated testbeds or synthetic data, thus limiting generalizability (Tooki & Popoola, 2024).

5. DISCUSSION

A detailed evaluation of 47 chosen studies of risk management methods for Cyber-Physical System (CPS) resilience reveals possible advantages and limitations in the following:

1. Traditional IT-centric risk assessment methodologies (STRIDE, CVSS) are widely utilized with CPS, but they have limitations in dealing with cyber-physical risk repercussions and operational restrictions.
2. While machine learning approaches have been proved to be useful for attack detection, there are still challenges with data availability, real-time processing, and resilience against adversarial assaults.
3. So far, few quantitative ways to measure resilience have been developed. majority of research still uses qualitative or semi-quantitative techniques.
4. Although there has been substantial progress in cascading failure analysis, these models use domain specific characteristics of the sectors and may not be generalizable.
5. Although the importance of social and environmental elements for CPS resilience is becoming more widely acknowledged, conventional risk management systems do not adequately account for them.

6. CONCLUSION AND FUTURE WORK

This systematic literature review examined 47 articles related to risk management models in multiple sectors with regard to CPS resilience. The review reveals a fast-moving, rapidly evolving field, with substantial advances in attack detection, risk assessment methods, and resilience frameworks. However, there are still significant gaps in cross-sector generalization, dynamic risk assessment, socio-technical integration, and real-world validation.

Additional studies should focus on:
Ensuring testbeds and benchmarks remain uniform so they may be compared across several investigations.

1. Examining social and environmental implications in quantitative risk models.
2. Improving real-time, adaptive risk assessment techniques.
3. Testing solutions on genuine CPS setups.
4. Research on AI-enhanced resilience mechanisms that are explainable.

As CPS expands into different sectors of critical infrastructure, demand for rigorous and detailed risk management will also expand. The review serves as a baseline for researchers and practitioners who wish to contribute to the development of CPS resilience engineering.

REFERENCE

Abshari, D., & Sridhar, M. (2026). Cyber-Physical Systems Security: A Comprehensive Review of Anomaly Detection Techniques. *Internet of Things*, *37*, 101938. https://doi.org/10.1016/j.iot.2026.101938

Adamos, K., Stergiopoulos, G., Karamousadakis, M., & Gritzalis, D. (2024). Enhancing attack resilience of cyber-physical systems through state dependency graph models. *International Journal of Information Security*, *23*(1), 187–198. https://doi.org/10.1007/s10207-023-00731-w

Aghazadeh Ardebili, A., Boscolo, M., Longo, A., Pourmadadkar, M., Ficarella, A., & Padoano, E. (2025). Resilience in Cyber-Physical Infrastructures: R-KPI prioritization, framework development, and case study insights. *Journal of Safety Science and Resilience*, *6*(3), 100194. https://doi.org/10.1016/j.jnlssr.2024.12.005

Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. *Applied Sciences*, *14*(24), 11807. https://doi.org/10.3390/app142411807

AlHarmali, A., Ali, S., Aman, W., & Hussain, O. (2024). Cyber Risk Assessment for Cyber-physical Systems: A Review of Methodologies and Recommendations for Improved Assessment Effectiveness. *Computational Science and Engineering*, 77–94. https://doi.org/10.5121/csit.2024.141608

Alrumaih, T. N. I., & Alenazi, M. J. F. (2025). ERINDA: A novel framework for Enhancing the Resilience of Industrial Networks against DDoS Attacks with adaptive recovery. *Alexandria Engineering Journal*, *121*, 248–262. https://doi.org/10.1016/j.aej.2025.02.042

Amro, A., Gkioulos, V., & Katsikas, S. (2023). Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework. *ACM Transactions on Privacy and Security*, *26*(2), 1–33. https://doi.org/10.1145/3571733

Atat, R., Ismail, M., & Serpedin, E. (2023). Cascading Failures Mitigation Strategy for Resilient Water Infrastructures*. *IFAC-PapersOnLine*, *56*(2), 4645–4650. https://doi.org/10.1016/j.ifacol.2023.10.977

Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*, *4*, 186–202. https://doi.org/10.1016/j.iotcps.2023.12.001

Canonico, R., Esposito, G., Navarro, A., Romano, S. P., Sperlí, G., & Vignali, A. (2025). An anomaly-based approach for cyber–physical threat detection using network and sensor data. *Computer Communications*, *234*, 108087. https://doi.org/10.1016/j.comcom.2025.108087

Cao, M., Ye, M., & Zino, L. (2025). Control of networked cyber–physical–human systems. *Nature Reviews Electrical Engineering*, *3*(1), 32–45. https://doi.org/10.1038/s44287-025-00224-z

Cao, Z., Zhao, H., Wang, Y., He, C., Zhou, D., & Han, X. (2025). A Resilience Quantitative Assessment Framework for Cyber–Physical Systems: Mathematical Modeling and Simulation. *Applied Sciences*, *15*(15), 8285. https://doi.org/10.3390/app15158285

Cassottana, B., Roomi, M. M., Mashima, D., & Sansavini, G. (2023). Resilience analysis of cyber-physical systems: A review of models and methods. *Risk Analysis*, *43*(11), 2359–2379. https://doi.org/10.1111/risa.14089

Chae, J., Lee, S., Jang, J., Hong, S., & Park, K.-J. (2023). A Survey and Perspective on Industrial Cyber-Physical Systems (ICPS): From ICPS to AI-Augmented ICPS. *IEEE Transactions on Industrial Cyber-Physical Systems*, *1*, 257–272. https://doi.org/10.1109/TICPS.2023.3323600

Cheimonidis, P., & Rantos, K. (2025). A novel proactive and dynamic cyber risk assessment methodology. *Computers & Security*, *154*, 104439. https://doi.org/10.1016/j.cose.2025.104439

El Qemmah, A., Casavola, A., & Tedesco, F. (2025). On the Detection of Deception Attacks and Resilience in Turn-Based Command Governors for Dynamically Decoupled Systems. *IFAC-PapersOnLine*, *59*(27), 196–201. https://doi.org/10.1016/j.ifacol.2025.12.102

Feng, Y., Huang, R., Zhao, W., Yin, P., & Li, Y. (2025). A survey on coordinated attacks against cyber–physical power systems: Attack, detection, and defense methods. *Electric Power Systems Research*, *241*, 111286. https://doi.org/10.1016/j.epsr.2024.111286

He, C., Xu, X., Jiang, H., Jiang, J., Liang, C., & Chen, T. (2026). A review of cyber-physical security for intelligent connected vehicles. *Chinese Journal of Mechanical Engineering*, *39*, 100178. https://doi.org/10.1016/j.cjme.2025.100178

Homaei, M., Tarif, M., Rodríguez, P. G., Caro, A., & Ávila, M. (2026). Causal Digital Twins for cyber–physical security in water systems: A framework for robust anomaly detection. *Machine Learning with Applications*, *23*, 100824. https://doi.org/10.1016/j.mlwa.2025.100824

Huang, H., Song, Y., Wei, Q., Geng, Y., & Wang, H. (2025). A comprehensive review of cyber-physical security risks in new power system. *Security and Safety*, *4*, 2025005. https://doi.org/10.1051/sands/2025005

Huang, S., Poskitt, C. M., & Shar, L. K. (2026). Security Modelling for Cyber-Physical Systems: A Systematic Literature Review. *ACM Transactions on Cyber-Physical Systems*, *10*(2), 1–29. https://doi.org/10.1145/3776549

Hujo-Lauer, D., Vogel-Heuser, B., Rupprecht, B., & Krüger, M. (2026). A Model-Based Decision Support for Field-to-Cloud Communication of Cyber-Physical Production Systems. *IEEE Transactions on Industrial Cyber-Physical Systems*, *4*, 201–212. https://doi.org/10.1109/TICPS.2026.3674578

Jiang, Y., Wu, S., Ma, R., Liu, M., Luo, H., & Kaynak, O. (2023). Monitoring and Defense of Industrial Cyber-Physical Systems Under Typical Attacks: From a Systems and Control Perspective. *IEEE Transactions on Industrial Cyber-Physical Systems*, *1*, 192–207. https://doi.org/10.1109/TICPS.2023.3317237

Kaliyaperumal, P., Karuppiah, T., Perumal, R., Thirumalaisamy, M., Balusamy, B., & Benedetto, F. (2025). Enhancing cybersecurity in Agriculture 4.0: A high-performance hybrid deep learning-based framework for DDoS attack detection. *Computers and Electrical Engineering*, *126*, 110431. https://doi.org/10.1016/j.compeleceng.2025.110431

Kampourakis, V., Gkioulos, V., & Katsikas, S. (2023). A systematic literature review on wireless security testbeds in the cyber-physical realm. *Computers & Security*, *133*, 103383. https://doi.org/10.1016/j.cose.2023.103383

Khattak, Z. H. (2024). Cybersecurity vulnerability and resilience of cooperative driving automation for energy efficiency and flow stability in smart cities. *Sustainable Cities and Society*, *106*, 105368. https://doi.org/10.1016/j.scs.2024.105368

Liu, C., Ye, J., Fang, G., Wang, D., Zhou, L., & Emadi, A. (2024). Resilience Framework for Power Electronic Systems Against Cyber-Physical Attacks: A Review. *IEEE Open Journal of Power Electronics*, 1–29. https://doi.org/10.1109/OJPEL.2024.3512452

Liu, R., Mangini, A. M., & Fanti, M. P. (2023). K-corruption Intermittent Attacks for Violating the Diagnosability. *IFAC-PapersOnLine*, *56*(2), 1847–1852. https://doi.org/10.1016/j.ifacol.2023.10.1900

Longo, A., Aghazadeh Ardebili, A., Lazari, A., & Ficarella, A. (2025). Cyber–Physical Resilience: Evolution of Concept, Indicators, and Legal Frameworks. *Electronics*, *14*(8), 1684. https://doi.org/10.3390/electronics14081684

Machaka, V., Figueroa-Lorenzo, S., Arrizabalaga, S., Elduayen-Echave, B., & Hernantes, J. (2025).
Assessing the impact of Modbus/TCP protocol attacks on critical infrastructure: WWTP case study. *Computers and Electrical Engineering*, *126*, 110485. https://doi.org/10.1016/j.compeleceng.2025.110485

Mouratidis, H., Islam, S., Santos-Olmo, A., Sanchez, L. E., & Ismail, U. M. (2023). Modelling language for cyber security incident handling for critical infrastructures. *Computers & Security*, *128*, 103139. https://doi.org/10.1016/j.cose.2023.103139

Rehman, Z., Gondal, I., Dong, H., Ge, M., Gregory, M. A., & Ul Haq, I. (2026). A robust eclipse attack detection framework for Ethereum networks. *Journal of Network and Computer Applications*, *246*, 104416. https://doi.org/10.1016/j.jnca.2025.104416

Segovia-Ferreira, M., Rubio-Hernan, J., Cavalli, A., & Garcia-Alfaro, J. (2024). A Survey on Cyber-Resilience Approaches for Cyber-Physical Systems. *ACM Computing Surveys*, *56*(8), 1–37. https://doi.org/10.1145/3652953

Sobb, T., Moustafa, N., & Turnbull, B. (2025). Responsible Resilience in Cyber–Physical–Social Systems: A New Paradigm for Emergent Cyber Risk Modeling. *Future Internet*, *17*(7), 282. https://doi.org/10.3390/fi17070282

Sobb, T., & Turnbull, B. (2025). CrowdStrike: Lessons in Mission Assurance to Build Resilience for Complex Cyber–Physical–Social Systems. *IEEE Access*, *13*, 205324–205337. https://doi.org/10.1109/ACCESS.2025.3634514

Soomro, I. A., Ur Rehman Khan, H., Hussain, S. J., Ashraf, Z., Alnfiai, M. M., & Alotaibi, N. N. (2024). Lightweight privacy-preserving federated deep intrusion detection for industrial cyber-physical system. *Journal of Communications and Networks*, *26*(6), 632–649. https://doi.org/10.23919/JCN.2024.000054

Tantawy, A., Erradi, A., Abdelwahed, S., & Shaban, K. (2020). Model-Based Risk Assessment for Cyber Physical Systems Security. *Computers & Security*, *96*, 101864. https://doi.org/10.1016/j.cose.2020.101864

Tooki, O. O., & Popoola, O. M. (2024). A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems. *Renewable Energy Focus*, *51*, 100628. https://doi.org/10.1016/j.ref.2024.100628

Verma, N., Kumar, N., Sheikh, Z. A., Koul, N., & Ashish, A. (2025). Machine Learning for the Cybersecurity of Robotic Cyber-Physical Systems: A Review. *Procedia Computer Science*, *259*, 1817–1826. https://doi.org/10.1016/j.procs.2025.04.137